Dc3 Digital Forensics Challenge

203 – Registry Analysis

Team Information

Team Name: AWGN

Results Email: [redacted]

Examination Time Frame: 10/1 to 10/21/08

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided registry files and USB Image files located in the **203_Registry_Analysis_Challenge2008** folder, which of the USB devices was attached to the suspect hard disk drive. Report the exact registry key path, any additional entry information, the detailed explanation of your process (software or technique) used to examine and detect the information, and the reason for your selections.

Points will be awarded for successfully identified USB device connected to the suspect hard disk drive, provided you supply a detailed methodology of how you determined your findings.

Total Weighted Points: 40 Total Points available per entry – Total 200 Points Available

1. **Answers –** Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer:

Points Awarded:

Date:

Review Period: to

Completed: □ Yes □ No □ Partial

Report of Examination

Challenge Number: 203 - Registry Analysis

Examiner: Graham Eschbacher

Loaded registry files into WRR.

usb_00*_org.fdisk identifies usb_001 and usb_002 as each having 1 FAT16 partition, and usb_003 as having 1 FAT32 partition. The command "mmls -t dos usb_00*.000" shows the start and end sectors of the partition, which can be extracted from the disk image using "dd". The command for this would be "dd if=usb_001.000 of=dos1.img bs=512 skip=32 count=1007584". Running the "file" command on each partition image reveals usb1 and usb2 to be Memorex TravelDrives, while usb3 is unlabeled. Several instances of "Memorex TD" appears in the registry, implying that either usb1 or usb2 was inserted. The serial numbers for the partition on drives 1, 2, and 3 are 0xf4d8dd43, 0xfd669053, and 0x7c6c0ed5.

None of these serial numbers shows up in the "System" registry file. A test of a personally owned usb drive shows that this serial number only shows up in the registry when it is plugged in. It is stored in Little Endian format in the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{Volume-ID}\Data. This 'Volume-ID' is also permanently located in MountPoints2, but there is no key that contains the partition's serial number.

Mounting each image showed the contents of them:

usb1
No Files

usb2
100.jpg 112.jpg 116.jpg 120.jpg 147.bmp 179.bmp 279.jpg 110.jpg 113.jpg 119.jpg 131.jpg 158.gif 238.jpg

usb3
100.jpg 187.jpg 238.jpg 279.jpg

The command "fsstat" confirms these numbers of files. Using "fls", deleted files were found on usb2 (command "fls -m / -r -f fat16 usb_002.img > usb2.fls"). Each deleted file could be extracted (usually partially) with a command similar to "icat -f fat16 usb_002.img 4 > d2-deleted/inode4._17.JPG"

A search of the registry for these images was unsuccessful. Also, searching Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count (after Rot-13 decryption) produced no results for any of these filenames.

If there is a serial number associated with the drive itself, and not just the partition, it is likely tied into the registry. This is due to the fact that you can have used a usb drive on a computer for some time, but when you insert another of the exact same brand and model, it still requires driver installation. This seems like the only definite way to identify the drive that was inserted, but I'm not sure where to get that info.

If I had to guess, I'd say USB1 was inserted because the registry clearly shows a Memorex TravelDrive being inserted at some point. Also, this drive contained no files, and the registry did not appear to have any references to the files on the other drive images.

Methodology / Notes Form

Challenge Number: 201 - Missing File Header Reconstruction

Tool Information

Type	Name	Publisher
○ Commercial ● Open Source	Notepad++	notepad-plus.sourceforge.net
● Commercial ○ Open Source	MiTeC Windows Registry Recovery (WRR)	www.mitec.cz
○ Commercial ● Open Source	Linux	
○ Commercial ● Open Source	The Sleuth Kit	www.sleuthkit.org
○ Commercial ○ Open Source		

Notes

For this challenge, I used several tools included in The Sleuth Kit for Linux to examine the usb drive images. I used WRR to examine the registry files. The main key that I found that could link the drive image to the computer was the serial number of the drive's partition. Unfortunately, this serial number is only present in the registry while the drive is physically inserted.

Page 1 of 1